CARRÉ DE POLYBE

Niveau : cycle 4, seconde.

Lien avec le programme : système de coordonnées-repérage, statistiques, fréquences.

Lien avec *Les maths au quotidien* : **Codages**.

Le **carré de Polybe** est une technique ancienne de transmission de messages, décrite pour la première fois vers 150 av. J.-C. par l'historien grec Polybe. Celle-ci a été utilisée par plusieurs civilisations de différentes manières tout au long de l'histoire.
C'est un chiffrement par substitution mono-alphabétique, les lettres du texte à coder sont remplacées par d'autres lettres de la façon suivante :

- Deux lettres différentes sont codées de façons différentes.
- La même lettre est toujours codée de la même façon.

Le principe de base consiste à placer les lettres de l'alphabet en ordre alphabétique dans un tableau carré de 5 cases de côté dont chaque ligne et chaque colonne sont numérotées, de haut en bas et de gauche à droite. Comme l'alphabet latin moderne comporte 26 lettres et que le carré possède seulement 25 cases, on attribue une même case à deux lettres proches, comme par exemple V et W (en français) ou bien I et J (en anglais).
Ensuite, pour chiffrer un mot, il faut trouver la paire de numéros correspondant à chaque lettre. Le premier chiffre est le numéro de la ligne et le second celui de la colonne. On ne tient pas compte des espaces ni de la ponctuation, et c'est le destinataire du message qui doit les replacer en tenant compte du sens.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V/W	X	Y	Z

1. Coder la phrase « J'adore les maths ».

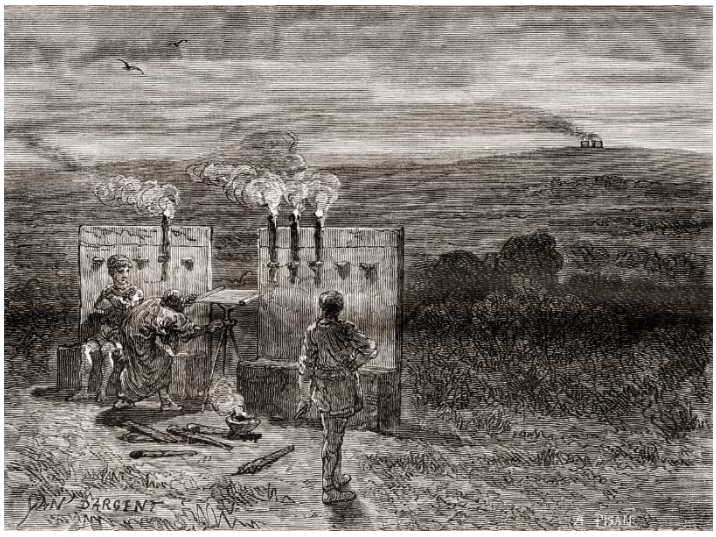
2. Décoder 35 34 34 15 52 35 24 45 12 24 15 34 42 51 11 52 15 13 31 15 13 35 15 51 43 31 15 44 44 15 34 45 24 15 31 15 44 45 24 34 52 24 44 24 12 31 15 41 35 51 43 31 15 44 54 15 51 53

Le carré de Polybe a été utilisé, entre autres, dans le domaine de la télégraphie (système de transmission rapide de messages sur de grandes distances, à l'aide de codes).

Son usage se justifiait par la nécessité de transmettre, entre villages, entre navires… un maximum d'informations avec un minimum d'objets.

Par exemple, des torches ont été utilisées. Sur la gravure ci-contre, le nombre de torches à gauche est le numéro de la ligne et le nombre de torches à droite est le numéro de la colonne dans le carré de Polybe.

3. Combien de torches étaient nécessaires pour coder les 25 lettres ?



Les Merveilles de la Science, Ecole Française, vers 1870

Un autre moyen de communication utilisant un carré de Polybe a été le « **code frappé »** (en anglais, ***tap code***). Plusieurs exemples dans l'histoire « récente » sont cités, dans un contexte politique.

Un premier se situe en Russie de la fin du XIX^{e} siècle jusqu'au début du XX^{e} siècle. Les nihilistes, opposants au régime tsariste et enfermés dans des prisons, utilisaient le principe du carré de Polybe pour communiquer entre eux en frappant contre les murs et les canalisations qui courraient dans la prison.

Le panneau ci-contre est apposé à l'entrée d'une des cellules du bastion Troubetskoï de la forteresse Pierre et Paul à Saint-Pétersbourg, que l'on peut visiter aujourd'hui. On reconnaît un carré de Polybe auquel on a ajouté une ligne non complète, ce qui donne 28 cases. En réalité l'alphabet cyrillique compte 33 symboles : les signes les moins fréquents ou inutiles pour la compréhension ont été supprimés.

Source : www.apprendre-en-ligne.net

Le carré de Polybe initial est un système de transmission « public », il n'y a pour ainsi dire aucune confidentialité quand on connait son principe. Le moyen le plus simple pour renforcer la méthode de chiffrement et de rendre un message plus confidentiel est sans aucun doute d'ajouter **une clé**.

La clé est un mot ou groupe de mots et il suffit d'ajouter chacune de ses lettres sans répétition au début du carré de Polybe. Ensuite, il faut ajouter les autres lettres de l'alphabet en ordre alphabétique. Par exemple, le carré de Polybe avec la clé MATHS AU QUOTIDIEN est représenté ci-contre.

	1	2	3	4	5
1	M	A	T	H	S
2	U	Q	O	I	D
3	E	N	B	C	F
4	G	J	K	L	P
5	R	V/W	X	Y	Z

4. Voici un texte codé avec une certaine clé (pas la précédente…) :

11 43 21 23 41 24 15 32 13 34 24 12 32 15 13 44 23 25 45 15 44 23 41 13 23 21 15 23 34 24 12 32 13 51 21 15 23 21 15 23 41 13

Quelle est la réponse ? Pour le savoir il faut le « précieux sésame ».

5. Le tableau ci-dessous exprime, **en pourcentages**, les fréquences moyennes, arrondies au dixième, des lettres utilisées dans les textes écrits en français.

A	B	C	D	E	F	G	H	I	J	K	L	M
7,8	1,1	3,5	3,9	15	1,2	0,9	0,7	7,7	0,5	0,1	5,7	3,2
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,2	5,6	3	1,5	6,8	8.1	7,4	6,5	1,7	0,1	0,4	0,3	0,1

En vous appuyant sur ce tableau, proposer un exemple de remplissage des 6 cases rouges d'un carré de Polybe qui minimise le nombre de coups à frapper sur les murs (pour la langue française).

	1	2	3	4	5
1					
2					
3					
4					
5					

Point info :

D'autres exemples de codes dérivés du carré de Polybe ont existé, utilisant une clé ou non :
- Des prisonniers américains, pendant la guerre du Viêt Nam, ont utilisé un code frappé dérivé du carré de Polybe. La technique a été introduite en juin 1965 par quatre prisonniers de guerre détenus dans la prison « Hỏa Lò » (ou « Maison Centrale », ironiquement « Hanoï Hilton »).
- Les Allemands ont utilisé, à partir de 1918, un chiffre inspiré du carré de Polybe, le GEDEFU18. Les coordonnées des lettres dans le carré n'étaient pas données par des chiffres, mais par les lettres ADFGX. Ces lettres ont été choisies de façon que leurs correspondances en morse soient très différentes les unes des autres, de façon à éviter les erreurs de transmission par radio (TSF). Mais dès juin 1918, les Allemands ajoutent la lettre V. Ils utilisèrent en effet pour leurs chiffrements deux modèles de carrés : l'un de 25 lettres, l'autre de 36 symboles, ce dernier étant obtenu par l'adjonction des 10 chiffres à un alphabet complet des 26 lettres latines.